tem **930** may be computer software designed for the purpose of managing databases. Typical examples of DBMSs include Oracle, DB2, Microsoft Access, Microsoft SQL Server, Postgres, MySQL and FileMaker. Examples of results as per embodiments described herein may include: metric (i.e. number of attackers that can reach a specific target); an attack path; part of an attack path; a collection of paths; an exploit; a condition-exploit pair; an exploit-condition pair; a table that describes an attack graph; a combination of the above; or the like.

[**0098**] The network may be reconfigured to decrease the likelihood of future attacks using the attack information learned from the result **950**.

[**0099**] The disclosed relational model enables interactive analysis of attack graphs for intrusion detection and prevention. It was shown that the complete attack graph may be generated as relational views. Analysis of the attack graph may thus be relational queries against such views. It was shown how to write relational queries for typical analyses previously studied in the literature. This novel approach made the analysis of attack graphs an interactive process similar to that in the decision support systems. As a side effect, the mature optimization techniques existing in most relational databases also improved the performance of the analysis.

[**0100**] The following references are provided as background to the above described principles to assist one skilled in the art understand the disclosure.

[**0101**] 1. P. Ammann, D. Wijesekera, and S. Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (*CCS'02*), pages 217-224, 2002.

[**0102**] 2. T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. MIT Press, 1990.

[**0103**] 3. F. Cuppens and A. Miege. Alert correlation in a cooperative intrusion detection framework. In *Proceedings of the* 2002 *IEEE Symposium on Security and Privacy* (*S&P'02*), pages 187-200, 2002.

[**0104**] 4. M. Dacier. Towards quantitative evaluation of computer security. Ph.D. Thesis, Institut National Polytechnique de Toulouse, 1994.

[**0105**] 5. R. Deraison. Nessus scanner, 1999. Available at http://www.nessus.org.

[**0106**] 6. D. Farmer and E. H. Spafford. The COPS security checker system. In *USENIX Summer*, pages 165-170, 1990.

[**0107**] 7. J. Gray, A. Bosworth, A. Bosworth, A. Layman, D. Reichart, M. Venkatrao, F. Pellow, and H. Pirahesh. Data cube: A relational aggregation operator generalizing group-by, cross-tab, and sub-totals. *Data Mining and Knowledge Discovery,* 1(1):29-53, 1997.

[**0108**] 8. S. Jajodia, S. Noel, and B. O'Berry. Topological analysis of network attack vulnerability. In V. Kumar, J. Srivastava, and A. Lazarevic, editors, *Managing Cyber Threats Issues, Approaches and Challenges*. Kluwer Academic Publisher, 2003.

[**0109**] 9. S. Jha, O. Sheyner, and J. M. Wing. Two formal analysis of attack graph. In *Proceedings of the* 15*th Computer Security Foundation Workshop* (*CSFW'02*), 2002.

[**0110**] 10. P. Ning, Y. Cui, and D. S. Reeves. Constructing attack scenarios through correlation of intrusion alerts. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (*CCS'02*), pages 245-254, 2002.

[**0111**] 11. S. Noel and S. Jajodia. Correlating intrusion events and building attack scenarios through attack graph distance. In *Proceedings of the* 20*th Annual Computer Security Applications Conference* (*ACSAC'04*), 2004.

[**0112**] 12. S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs. Efficient minimum-cost network hardening via exploit dependency grpahs. In *Proceedings of the* 19*th Annual Computer Security Applications Conference* (*ACSAC'03*), 2003.

[**0113**] 13. R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Trans. Software Eng.,* 25(5):633-650, 1999.

[**0114**] 14. C. Phillips and L. Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the New Security Paradigms Workshop* (*NSPW'98*), 1998.

[**0115**] 15. C. R. Ramakrishnan and R. Sekar. Model-based analysis of configuration vulnerabilities. *Journal of Computer Security,* 10(1/2):189-209, 2002.

[**0116**] 16. R. Ritchey and P. Ammann. Using model checking to analyze network vulnerabilities. In *Proceedings of the* 2000 *IEEE Symposium on Research on Security and Privacy* (*S&P'00*), pages 156-165, 2000.

[**0117**] 17. R. Ritchey, B. O'Berry, and S. Noel. Representing TCP/IP connectivity for topological analysis of network security. In *Proceedings of the* 18*th Annual Computer Security Applications Conference* (*ACSAC'02*), page 25, 2002.

[**0118**] 18. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing. Automated generation and analysis of attack graphs. In *Proceedings of the* 2002 *IEEE Symposium on Security and Privacy* (*S&P'02*), pages 273-284, 2002.

[**0119**] 19. L. Swiler, C. Phillips, D. Ellis, and S. Chakerian. Computer attack graph generation tool. In *Proceedings of the DARPA Information Survivability Conference & Exposition II* (*DISCEX'01*), 2001.

[**0120**] 20. L. Wang, A. Liu, and S. Jajodia. An efficient and unified approach to correlating, hypothesizing, and predicting intrusion alerts. In Proceedings of the 10th European Symposium on Research in Computer Security (ESORICS 2005), pages 247-266, 2005.

[**0121**] 21. D. Zerkle and K. Levitt. Netkuang—a multi-host configuration vulnerability checker. In *Proceedings of the 6th USENIX Unix Security Symposium* (*USENIX'96*), 1996.

[**0122**] While various embodiments have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in